

AN: Präsident des Oberlandesgerichts Düsseldorf

1. ABSENDER:

Mark L. Whitaker
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1888
USA

2. ZENTRALBEHÖRDE DES
ERSUCHTEN STAATES:

Der Präsident
des Oberlandesgerichts Düsseldorf
Cecilienallee 3
40474 Düsseldorf
Deutschland

3. PERSONEN, AN DIE DAS AUSGEFÜHRTE ERSUCHEN ZURÜCKGEGEBEN WERDEN SOLL:
FOERSTER LLP

Mark L. Whitaker
MORRISON &
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1888
USA

Tharan Gregory Lanier
JONES DAY
555 California Street, 26th Floor
San Francisco, CA 94104
USA

4. DATUM, BIS ZU DEM DIE ERSUCHENDE BEHÖRDE DEN EINGANG DER ANTWORT
AUF DAS SCHREIBEN DES ERSUCHENS ANFORDERT:

Dieses Ersuchen ist von dringender Natur, da die Ermittlungen in dieser Angelegenheit am 15. Januar 2021 enden werden. Da noch weniger als ein Jahr für die Ermittlungen verbleibt, bleibt Teradata keine andere Wahl, als das deutsche Rechtssystem um Unterstützung zu bitten, um diese wichtigen Informationen zu erhalten.

Entsprechend Artikel 3 des Haager Übereinkommens vom 18. März 1970 über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen ("Haager Beweisaufnahmeübereinkommen") hat der unterzeichnende Antragsteller das Recht, folgenden Antrag zu stellen:

5(a) ANFORDERNDE JUSTIZBEHÖRDE: Der Ehrenwerte Joseph C. Spero
Staaten
Staaten für den

Oberster Magistratsrichter der Vereinigten
Bundesbezirksgericht der Vereinigten
Northern District of California
San Francisco Courthouse

450 Golden Gate Avenue,
San Francisco, CA 94102
USA

(b) AN DIE ZUSTÄNDIGE BEHÖRDE VON: Deutschland

(c) FALLNAME UND -NUMMER: TERADATA CORPORATION,
TERADATA US, INC., und TERADATA
OPERATIONS, INC. v. SAP SE, SAP
AMERICA, INC., und SAP LABS, LLC,

Fall Nr. 3:18-cv-03670

6. NAMEN UND ADRESSEN DER PARTEIEN UND VERTRETER:

(a) Kläger 1: Teradata Corporation
17095 Via del Campo
San Diego, CA 92127
USA

Kläger 2: Teradata US, Inc.
17095 Via del Campo
San Diego, CA 92127
USA

Kläger 3: Teradata US, Inc.
17095 Via del Campo
San Diego, CA 92127
USA

Syndizi der Kläger 1, 2 und 3: Mark L. Whitaker
Daniel P. Muino
G. Brian Busey
Mary Prendergast
Fahd H. Patel
Michelle L. Yocum
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1888
USA

(b) Angeklagter 1: SAP SE
Dietmar-Hopp-Allee 16
Walldorf, 69190

Deutschland

Angeklagter 2:

SAP America, Inc.
3999 West Chester Pike
Newton Square, PA 19073
USA

Angeklagter 3:

SAP Labs, LLC
3410 Hillview Avenue
Palo Alto, CA 94304
USA

Syndizi der Angeklagten 1, 2 und 3:

Tharan Gregory Lanier
Nathaniel P. Garrett
Joshua L. Fuchs
Joseph M. Beauchamp
JONES DAY
555 California Street, 26th Floor
San Francisco, CA 94104
USA

Kenneth A. Gallo
David J. Ball
William B. Michael
PAUL WEISS
2001 K Street NW
Washington, DC 20006-1047
USA

Kristin L. Cleveland
John D. Vandenberg
KLARQUIST SPARKMAN, LLP
121 SW Salmon Street, Suite 1600
Portland, OR 97204
USA

7. ART DES VERFAHRENS UND ZUSAMMENFASSUNG DER KLAGE UND DER GEGENKLAGE:

(a) Art des Verfahrens. Bei dem Verfahren, für das die Antragsteller mündliche Zeugenaussagen von den in Abschnitt 9 unten aufgeführten Zeugen beantragen, handelt es sich um eine Zivilklage, die von Teradata Corporation, Teradata US Inc. und Teradata Operations, Inc. (zusammen "Teradata" genannt) gegen SAP SE, SAP America Inc. und SAP Labs, LLC (zusammen "SAP" genannt) eingereicht wurde. Dieser Fall ist sowohl zivil- als auch handelsrechtlicher Natur und beinhaltet weder einen Rechtsstreit über eine strafrechtliche, innerstaatliche oder familienrechtliche Frage noch die Rückforderung einer Steuer.

(b) Zusammenfassung der Klage/Gegenklage. Die Klage von Teradata stützt sich auf Ansprüche wegen (i) missbräuchlicher Verwendung von Geschäftsgeheimnissen gemäß US-amerikanischem Bundesgesetz (18 U.S.C. § 1836, *et seq.*); (ii) missbräuchlicher Verwendung von Geschäftsgeheimnissen gemäß kalifornischem Staatsgesetz (Cal. Civil Code § 3426, *et seq.*); (iii) Verletzung des Urheberrechts gemäß 17 U. S.C. § 501; (iv) unrechtmäßige Bindung gemäß 15 U.S.C. §§ 1, 14; und (v) versuchte Monopolisierung gemäß 15 U.S.C. § 2 durch das mutmaßlich wettbewerbswidrige Verhalten von SAP gegenüber Teradata und den mutmaßlichen Missbrauch des geistigen Eigentums von Teradata. In der Antwort von SAP werden diese Vorwürfe bestritten, und in den Gegenklagen von SAP werden Ansprüche wegen Verletzung von fünf SAP-Patenten gemäß 35 U.S.C. § 271 durch die mutmaßliche Nutzung von geistigem Eigentum von SAP seitens Teradata erhoben.

Gegenstand des Falles ist Unternehmenssoftware. Die Parteien gingen 2008 ein Joint Venture ein, das es dem SAP-Produkt "Business Warehouse" ermöglichte, das Produkt "Teradata Database" von Teradata zu nutzen. Im Jahr 2011 veröffentlichte SAP ein eigenes Produkt namens "HANA", das mit dem Produkt von Teradata konkurrierte. Teradata ist der Ansicht, dass SAP das durch das Joint Venture erworbene geistige Eigentum von Teradata zur Entwicklung des SAP-Produkts "HANA" verwendet hat und dass SAP versucht hat, Kunden dazu zu nötigen, das Produkt "HANA" und nicht das Produkt "Teradata Database" zu verwenden, in einer Weise, die gegen das US-amerikanische Kartellrecht verstößt. SAP ist der Ansicht, dass das Produkt Teradata Database gegen die Patentrechte von SAP verstößt.

Während des Joint Ventures beauftragte SAP die Infolytics AG mit der Entwicklung einer Software, die das SAP-Produkt Business Warehouse mit dem Produkt Teradata Database verknüpft. Einige Mitarbeiter von Infolytics erhielten "@sap.com"-E-Mail-Adressen, was nach Angaben von SAP Bestandteil des begrenzten "Vertragspartner-Benutzer"-Zugriffs dieser Mitarbeiter auf das SAP-Netzwerk war. Zu den Infolytics-Mitarbeitern, die SAP-E-Mail-Adressen erhielten, gehörten Thomas Anhaus und Fekke Fekkes.

8. ZU ERLANGENDES BEWEISMATERIAL:

Die ersuchende Justizbehörde bittet die deutsche Zentralbehörde höflichst, die Zeugen Thomas Anhaus, Fekke Fekkes, Jürgen Hoehe, Arthur Janowitz, Ralf Scheurer und Gerhard Brunnbauer sowie möglicherweise weitere Mitarbeiter und Führungskräfte der Infolytics AG, die über relevante Informationen verfügen, vor Gericht erscheinen und aussagen zu lassen. Die Infolytics AG ist die Firma, für die die Zeugen Thomas Anhaus, Fekke Fekkes, Jürgen Höhe, Arthur Janowitz, Ralf Scheurer und Gerhard Brunnbauer zumindest während des Brückenprojektes gearbeitet haben. Diese Zeugenaussagen sollen im Prozess als Beweismittel dienen und werden in Abschnitt 10 weiter unten ausführlicher erläutert.

Die ersuchende Justizbehörde hat ferner bestimmt, dass die hierin ersuchten Zeugenaussagen zur Verwendung in der Gerichtsverhandlung anstelle eines persönlichen Erscheinens dieser Zeugen aufgenommen werden können. Nach Prüfung der zur Unterstützung des Antrags auf Erteilung dieses Ersuchens vorgelegten Schriftstücke ist dieses Gericht davon überzeugt, dass das Ersuchen notwendig und zweckmäßig ist, um Beweise vorzulegen, die diesem Gericht bei der Lösung bestimmter Fragen helfen, die während der Verhandlung der Angelegenheit zu klären sind.

9. IDENTITÄT UND ADRESSEN DER ZU VERNEHMENDEN PERSONEN:

Thomas Anhaus
Hesterstr. 23, 58135 Hagen
Deutschland

Fekke Fekkes
Bonner Strasse 484-486, 50968 Köln
Deutschland

Juergen Hoehe
Agrippinaufer 4, 50678 Köln
Deutschland

Arthur Janowitz
Weiherstr. 6, 52152 Simmerath
Deutschland

Ralf Scheurer
Homburger Str. 22, 50969 Köln
Deutschland

Gerhard Brunnbauer
Bonner Strasse 484-486, 50968 Köln
Deutschland

10. DARLEGUNG DES GEGENSTANDS, ÜBER WELCHEN DER ZEUGE VERNOMMEN WERDEN SOLL:

Vor diesem Gericht wurde vorgebracht, dass die Vernehmungen von Thomas Anhaus, Fekke Fekkes, Jürgen Höhe, Arthur Janowitz, Ralf Scheurer und Gerhard Brunnbauer, Mitarbeiter und Manager von Infolytics, die gegenwärtig in Deutschland wohnhaft sind, für die ordnungsgemäße Klärung der zwischen den Parteien strittigen Fragen erforderlich sind. Teradata möchte die Aussage von Thomas Anhaus zu den zentralen Fragen der mutmaßlichen missbräuchlichen Verwendung von Geschäftsgeheimnissen von Teradata während des Brückenprojekts aufnehmen. Herr Anhaus war während des Brückenprojekts Mitglied des Teams "Project Steering SAP MaxDB Bridge" und des Teams "MaxDB Kernel & Interfaces". Herr Anhaus war an der Entwicklung einer Loading Solution beteiligt, um Daten von einem SAP-Produkt zu Teradata zu übertragen. Herr Anhaus soll bei der Entwicklung dieser Anwendung mit sensiblen Teradata-Informationen, einschließlich Quellcode, gearbeitet haben. Teradata möchte auch die Zeugenaussage von Fekke Fekkes zur zentralen Frage der mutmaßlichen missbräuchlichen Verwendung von Geschäftsgeheimnissen von Teradata während des Brückenprojekts aufnehmen. Herr Fekkes war während des Brückenprojekts Mitglied des Teams "Project Steering SAP MaxDB Bridge" und des Teams "BW Interface". Herr Fekkes war an der Prüfung der Leistung des Brückenprojekts beteiligt. Teradata möchte auch die Zeugenaussagen

der Herren Hoehe, Janowitz, Scheurer und Brunnbauer aufnehmen, die alle am Brückenprojekt beteiligt waren.

Der Umfang der angeforderten Beweise ist spezifisch für Angelegenheiten innerhalb der persönlichen Kenntnisse der Herren Anhaus, Fekkes, Hoehe, Janowitz, Janowitz, Scheurer und/oder Brunnbauer während ihrer Tätigkeit bei Infolytics und der Arbeit, die sie dort im Rahmen des Brückenprojekts geleistet haben. Insbesondere geht es um die Rolle dieser Personen während des Brückenprojekts, den mutmaßlichen Zugang zu und den Umgang mit geschützten Informationen von Teradata und die Art der Beziehung der Infolytics AG zu Teradata im Allgemeinen, zu SAP im Allgemeinen und insbesondere zu den Projekten BW und HANA von SAP. Die angeforderten Dokumente beziehen sich auf dieselben.

11. DOKUMENTE ODER ANDERES ZU ÜBERPRÜFENDES MATERIAL: Separates Antragsschreiben.

12 und 13. BESONDERE VERFAHREN, DIE GEMÄSS ARTIKEL 3 und 9 DES ÜBEREINKOMMENS ERFORDERLICH SIND:

Allgemeine Verfahrensweisen:

Für den Fall, dass die Beweisaufnahme in der oben genannten Art und Weise mit den Gesetzen der Bundesrepublik Deutschland unvereinbar ist oder aufgrund interner Praxis und Verfahren oder praktischer Schwierigkeiten in Deutschland nicht durchgeführt werden kann, wird hochachtungsvoll darum gebeten, dass die Beweisaufnahme in einer ähnlichen Art und Weise durchgeführt wird, wie sie in den Gesetzen der Bundesrepublik Deutschland für die formelle Aufnahme einer mündlichen Zeugenaussage vorgesehen ist.

Es wird höflichst darum gebeten, dass: (a) die mündliche Zeugenaussage unter Eid oder eidesstattlicher Versicherung einer nach deutschem Recht zur Eidesleistung befugten Behörde oder Person erfolgt; (b) die Zeugenvernehmung in englischer Sprache nach direkter mündlicher Vernehmung und Kreuzverhör durch einen Rechtsbeistand für die Parteien in dem laufenden Verfahren erfolgt, es sei denn, der Zeuge beantragt, dass die Zeugenaussage in deutscher Sprache aufgenommen wird; in diesem Fall stellt der Rechtsbeistand von Teradata einen Übersetzer in dieser Sprache zur Verfügung; (c) die Aussage des Zeugen auf eine wörtliche Abschrift durch einen qualifizierten Reporter oder Stenographen reduziert wird; (d) nach Abschluss der Zeugenvernehmung die Abschrift vom Zeugen vereidigt und an die in Abschnitt 3 oben genannte(n) Person(en) zurückgegeben wird; und (e) die Parteien die Zeugenvernehmung auf Video aufzeichnen dürfen. Darüber hinaus wird höflichst darum gebeten, dass die Zentralbehörde Deutschlands dem Zeugen die Benachrichtigung gemäß deutschem Recht zustellt.

Vertraulichkeit der Zeugenaussagen:

Alle vertraulichen Informationen, die in diesem Rechtsstreit offenbart werden, unterliegen einer vereinbarten Schutzanordnung ("Schutzanordnung", beigefügt als Anlage 1), die dazu bestimmt ist, die vorliegenden Unternehmen vor der unbefugten Nutzung und/oder Offenlegung von Geschäftsgeheimnissen und anderen vertraulichen Informationen zu schützen. Die Schutzanordnung sieht Folgendes vor: "[J]ede Nichtpartei, die im Rahmen des Rechtsstreits Dokumente oder Informationen vorlegt, kann die in dieser Schutzanordnung vorgesehene

vertrauliche Behandlung in Anspruch nehmen, indem sie eine Kopie dieser Schutzanordnung unterschreibt und diese allen beteiligten Anwälten zustellt. (Anhang 1 unter ¶ 29.) Die Schutzanordnung umfasst in ihrem Geltungsbereich alle Informationen, die durch eidesstattliche Aussagen offenbart werden. (*Id.* unter ¶ 2.) Dementsprechend hat dieses Gericht der Infolytics AG und ihren Mitarbeitern und Managern ausdrücklich das Recht eingeräumt, alle vertraulichen Informationen, die in Beantwortung dieses Antrags erteilt wurden, als "HOCH VERTRAULICH" oder "NUR FÜR EXTERNE ANWÄLTE" unter der Schutzanordnung zu bezeichnen. Der Zugang zu Informationen, die als "HOCH VERTRAULICH" bezeichnet werden, ist in der Regel auf zwei interne Rechtsanwälte jeder Partei beschränkt, wohingegen Informationen, die als "NUR FÜR EXTERNE ANWÄLTE" ausgewiesen sind, von den externen Anwälten jeder Partei und anderen, die eng in das Gerichtsverfahren involviert sind, eingesehen werden können. (*Id.* unter ¶ 7.)

14. BITTE UM BENACHRICHTIGUNG ÜBER ZEIT UND ORT FÜR DIE AUSFÜHRUNG DES ERSUCHENS SOWIE IDENTITÄT UND ANSCHRIFT DER ZU BENACHRICHTIGENDEN PERSONEN:

Da es keine Abmachung darüber gibt, dass die Herren Anhaus, Fekkes, Hoehe, Janowitz, Scheurer und Brunnbauer außerhalb Deutschlands zur Zeugenaussage in dieser Angelegenheit erscheinen, wird höflichst darum gebeten, dass die Zentralbehörde Deutschlands den Zeitpunkt für die Zeugenaussage im Juni 2020 oder zu einem späteren Zeitpunkt, wie von den Parteien vereinbart, festlegt. Die Parteien werden sich untereinander und mit den Zeugen beraten, um einen für beide Seiten annehmbaren Zeitrahmen festzulegen. Die Parteien haben vereinbart, dass für jeden Zeugen zunächst Teradata den Zeugen befragt und dass SAP die gleiche Zeit für das Kreuzverhör des Zeugen zur Verfügung steht. Sobald der Zeitpunkt und der Ort für die Durchführung der Anfrage von der zuständigen Behörde festgelegt sind, wird um Zustellung einer Benachrichtigung an die folgenden Empfänger gebeten:

Mark L. Whitaker
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1888
USA

Tharan Gregory Lanier
JONES DAY
555 California Street, 26th Floor
San Francisco, CA 94104
USA

15 und 16. NICHT ZUTREFFEND.

17. GEBÜHREN UND KOSTEN:

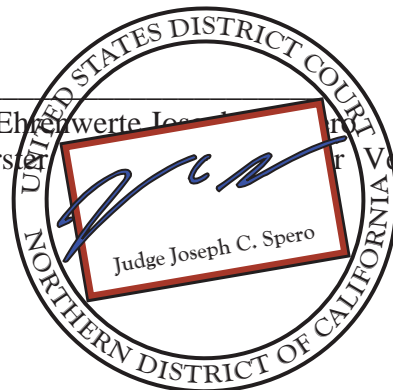
Die gegebenenfalls gemäß Artikel 14 Absatz 2 oder Artikel 26 der Übereinkunft erstattungsfähigen Gebühren und Kosten werden von Teradata getragen.

DATUM DES ERSUCHENS: _____ April 28 _____, 2020

UNTERSCHRIFT UND STEMPEL DER ERSUCHENDEN BEHÖRDE:

Staaten

Der Ehrenwerte Le...
Oberster ... r Vereinigten



ANHANG 1

Mark L. Whitaker (*Pro Hac Vice*)
MWhitaker@mofo.com
Daniel P. Muino (CA SBN 209624)
DMuino@mofo.com
G. Brian Busey (*Pro Hac Vice*)
GBusey@mofo.com
Mary Prendergast (CA SBN 272737)
MPrendergast@mofo.com
Fahd H. Patel (*Pro Hac Vice*)
FPatel@mofo.com
Corinna J. Alanis (CA SBN 287164)
CAlanis@mofo.com
MORRISON & FOERSTER LLP
2000 Pennsylvania Ave., NW
Washington, D.C. 20006-1888
Telefon: 202.887.1500
Faksimile: 202.887.0763

Bryan Wilson (CA SBN 138842)
BWilson@mofo.com MORRISON
& FOERSTER LLP
755 Page Mill Road
Palo Alto, California 94304-1018
Telefon: 650.813.5600
Faksimile: 650.494.0792

Anwälte der Kläger
TERADATA CORPORATION,
TERADATA US, INC., UND
TERADATA OPERATIONS, INC.

Tharan Gregory Lanier (Anwaltskammer Nr.
138784)
tglanier@JonesDay.com
Nathaniel P. Garrett (Anwaltskammer Nr.
248211)
ngarrett@JonesDay.com
Joshua L. Fuchs (*Pro Hac Vice*)
jlfuchs@JonesDay.com
JONES DAY
555 California Street, 26th Floor
San Francisco, CA 94104
Telefon: +1.415.626.3939
Faksimile: +1.415.875.5700

Kenneth A. Gallo (*Pro Hac Vice*)
kgallo@paulweiss.com
David J. Ball (*Pro Hac Vice*)
dball@paulweiss.com
William B. Michael (*Pro Hac Vice*)
wmichael@paulweiss.com
PAUL, WEISS, RIFKIND, WHARTON &
GARRISON LLP
2001 K Street NW
Washington, DC 20006-1047
Telefon: +1.202.223.7356
Faksimile: +1.202.204.7356

Anwälte der Angeklagten
SAP SE,
SAP AMERICA, INC., UND
SAP LABS, LLC

BUNDESBEZIRKSGERICHT DER VEREINIGTEN STAATEN
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

TERADATA CORPORATION, TERADATA US,
INC., und TERADATA OPERATIONS,
INC.,

Kläger,

SAP SE, SAP AMERICA, INC., und SAP
LABS, LLC,

Angeklagte.

Fall Nr. 3:18-cv-03670-WHO (EDL)

VEREINBARTE [GEPLANTE]
SCHUTZANORDNUNG

1. ABSICHTEN UND BESCHRÄNKUNGEN

Im Rahmen dieses Verfahrens werden wahrscheinlich vertrauliche, geschützte oder private Informationen ermittelt und vorgelegt, für die ein besonderer Schutz vor öffentlicher Offenlegung und vor der Verwendung für andere Zwecke als die Verfolgung dieses Rechtsstreits gerechtfertigt sein kann. In diesem Sinne vereinbaren die Parteien hiermit und ersuchen das Gericht, die folgende vereinbarte Schutzanordnung zu erlassen. Die Parteien erkennen an, dass diese Anordnung keinen pauschalen Schutz für alle Offenlegungen oder Entscheidungen über die Offenlegung gewährt und dass der Schutz, den sie vor der öffentlichen Offenlegung und Nutzung gewährt, sich nur auf die begrenzten Informationen oder Gegenstände erstreckt, die nach den geltenden Rechtsgrundsätzen zur vertraulichen Behandlung berechtigt sind. Die Parteien erkennen ferner, wie in Abschnitt 13.4 unten dargelegt, an, dass diese Vereinbarte Schutzanordnung sie nicht berechtigt, vertrauliche Informationen unter Verschluss einzureichen; die lokale Zivilprozessregel 79-5 legt die Verfahrensweisen fest, die befolgt werden müssen, und die Standards, die angewendet werden, wenn eine Partei beim Gericht die Erlaubnis beantragt, Material unter Verschluss einzureichen.

2. DEFINITIONEN

2.1 Anfechtende Partei: eine Vertragspartei oder Nichtvertragspartei, die die Benennung von Informationen oder Gegenständen im Rahmen dieses Beschlusses anfechtet.

2.2 "VERTRAULICHE" Informationen oder Gegenstände: Informationen (unabhängig davon, wie sie erzeugt, gespeichert oder gewartet werden) oder materielle Dinge, die für den Schutz nach der Zivilprozessordnung (Federal Rule of Civil Procedure) 26(c) in Frage kommen.

2.3 Syndikus (ohne Zusatz): Externer Syndikus des Protokolls und Syndikus des Hauses (sowie deren Hilfspersonal).

2.4 Benannter Syndikus des Hauses: Syndikus des Hauses, der Zugang zu "HOCH VERTRAULICHEN - NUR FÜR ANWÄLTE EINSEHBARE" Informationen in dieser Rechtssache ersucht, die das "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" unterzeichnet haben. Jede Seite (Kläger auf der einen Seite und Angeklagte auf der anderen) kann bis zu - aber nicht mehr als - vier (4) Syndizi des Hauses als benannte Syndizi des Hauses in diesem Rechtsstreit benennen.

2.5 Benennende Partei: eine Vertragspartei oder Nichtvertragspartei, die Informationen oder Gegenstände, die sie in Offenlegungen oder in Antworten auf Entdeckungen vorlegt, als "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" bezeichnet.

2.6 Offenlegungs- oder Beweismaterial: alle Gegenstände oder Informationen, unabhängig vom Medium oder der Art und Weise, in der sie erzeugt, gespeichert oder bereit gehalten werden (einschließlich u.a. Zeugenaussagen, Niederschriften und handfeste Dinge), die in Offenlegungen oder Antworten auf eine Entdeckung in dieser Angelegenheit vorgelegt oder generiert werden.

2.7 Experte: eine Person mit speziellen Kenntnissen oder Erfahrungen in einer für den Rechtsstreit relevanten Angelegenheit, die (1) von einer Partei oder ihrem Rechtsbeistand als Sachverständiger oder Berater in diesem Verfahren beauftragt wurde, (2) kein gegenwärtiger Angestellter einer Partei oder eines Konkurrenten einer Partei ist (zur Vermeidung von Konflikten bezieht sich dieser Unterabschnitt (2) nur auf einen gegenwärtigen Angestellten und nicht auf einen gegenwärtigen Berater eines Konkurrenten einer Partei), und (3) zum Zeitpunkt der Beauftragung nicht beabsichtigt ist, Angestellter einer Partei oder eines Konkurrenten einer Partei zu werden.

2.8 "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBARE" Informationen oder Gegenstände: Äußerst sensible "vertrauliche Informationen oder Gegenstände", deren Offenlegung gegenüber einer anderen Vertragspartei oder Nichtvertragspartei ein erhebliches Risiko eines ernsthaften Schadens schaffen würde, der durch weniger restriktive Mittel nicht vermieden werden könnte.

2.9 "HOCH VERTRAULICH - QUELLCODE" Informationen oder Gegenstände: Äußerst sensible "Vertrauliche Informationen oder Gegenstände", die Computercode darstellen, oder detaillierte Beschreibungen von Computercode, die die wesentlichen Bestandteile von Computercode offenbaren könnten, die die Algorithmen oder die Struktur von Software- oder Hardware-Designs definieren oder anderweitig detailliert beschreiben, deren Offenlegung gegenüber einer anderen Vertragspartei oder Nichtvertragspartei ein erhebliches Risiko eines ernsthaften Schadens schaffen würde, der durch weniger restriktive Mittel nicht vermieden werden könnte.

2.10 Syndikus des Hauses: Rechtsanwälte, die Angestellte einer an diesem Verfahren beteiligten Partei sind. Syndikus des Hauses beinhaltet nicht den externen Syndikus des Protokolls oder andere externe Anwälte.

2.11 Nichtpartei: Jede natürliche Person, Personengesellschaft, Körperschaft, Vereinigung oder andere juristische Person, die nicht als Partei dieses Verfahrens genannt wird.

2.12 Externer Syndikus des Protokolls: Anwälte, die nicht Angestellte einer an diesem Verfahren beteiligten Partei sind, die jedoch beauftragt sind, eine an diesem Verfahren beteiligte Partei zu vertreten oder zu beraten, und die in diesem Verfahren im Namen dieser Partei aufgetreten sind oder die mit einer Anwaltskanzlei zusammenarbeiten, die im Namen dieser Partei aufgetreten ist.

2.13 Partei: Jede an diesem Verfahren beteiligte Partei, einschließlich aller ihrer leitenden Angestellten, Direktoren, Mitarbeiter, Berater, beauftragten Experten, beteiligten Vorgänger, Rechtsnachfolger, Tochtergesellschaften, Muttergesellschaften, Niederlassungen, verbundenen Unternehmen, Abteilungen und externen Anwälte (sowie deren Hilfspersonal).

2.14 Vorlegende Partei: Eine Partei oder Nichtpartei, die im Rahmen dieses Verfahrens Offenlegungs- oder Beweismaterial vorlegt.

2.15 Professionelle Dienstleister: Personen oder Organisationen, die Dienstleistungen zur Unterstützung bei Rechtsstreitigkeiten anbieten (z. B. Fotokopieren, Videoaufzeichnung, Übersetzung, Vorbereitung von Exponaten oder Vorführungen und Organisation, Speicherung oder Abruf von Daten in jeglicher Form oder auf jeglichem Medium) sowie deren Mitarbeiter und Subunternehmer.

2.16 Geschütztes Material: Jegliches Offenlegungs- oder Beweismaterial, das als "VERTRAULICH", als "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder als "HOCH VERTRAULICH - QUELLCODE" bezeichnet wird.

2.17 Empfangende Partei: Eine Partei, die Offenlegungs- oder Beweismaterial von einer vorliegenden Partei erhält.

3. GELTUNGSBEREICH

Der durch diese Vereinbarung und Verfügung gewährte Schutz erstreckt sich nicht nur auf geschütztes Material (wie oben definiert), sondern auch auf (1) alle aus geschütztem Material kopierten oder extrahierten Informationen, die geschütztes Material offenbaren könnten; (2) alle Kopien, Auszüge, Zusammenfassungen oder Sammlungen von geschütztem Material, die geschütztes Material offenbaren könnten; und (3) alle Zeugenaussagen, Gespräche oder Präsentationen von Parteien oder ihren Syndizi, die geschütztes Material offenbaren könnten. Der durch diese Vereinbarung und Verfügung gewährte Schutz erstreckt sich jedoch nicht auf die folgenden Informationen: (a) Sämtliche Informationen, die zum Zeitpunkt der Offenlegung gegenüber einer empfangenden Partei öffentlich bekannt sind oder nach ihrer Offenlegung gegenüber einer empfangenden Partei infolge einer Veröffentlichung, die keinen Verstoß gegen diese Anordnung darstellt, einschließlich der Tatsache, dass sie durch ein Gerichtsverfahren oder auf andere Weise Teil der öffentlichen Unterlagen werden; und (b) Sämtliche Informationen, die der empfangenden Partei vor der Offenlegung bekannt waren oder die die empfangende Partei nach der Offenlegung von einer Quelle erhalten hat, die die Informationen rechtmäßig und ohne Verpflichtung zur Vertraulichkeit gegenüber der benennenden Partei erhalten hat.

Ferner soll nichts in dieser Vereinbarung und Verfügung den externen Syndikus oder den Benannten Syndikus des Hauses einer Partei daran hindern, allgemeine Ratschläge zu erteilen, die keine spezifischen Einzelheiten des geschützten Materials offenlegen. Jegliche Verwendung von geschütztem Material bei der Verhandlung wird durch eine separate Vereinbarung oder Verfügung geregelt.

4. DAUER

Auch nach endgültiger Beilegung dieses Rechtsstreits bleiben die durch diesen Beschluss auferlegten Geheimhaltungspflichten in Kraft, bis eine benennende Partei schriftlich etwas anderes vereinbart oder ein Gerichtsbeschluss etwas anderes anordnet. Das Gericht bleibt auch nach der endgültigen Entscheidung in dieser Angelegenheit für die Verhandlung und Beilegung von Rechtsstreitigkeiten, die sich aus dieser Verfügung ergeben, zuständig. Als endgültige Entscheidung gilt (1) die Abweisung aller Ansprüche und Einsprüche in dieser Klage, mit oder ohne Präjudiz, und (2) das endgültige Urteil nach Abschluss und Erschöpfung aller Berufungen, Wiederaufnahmen, Mahnungen, Prozesse oder Überprüfungen dieser Klage, einschließlich der Fristen für die Einreichung von Anträgen oder Anträgen auf Fristverlängerung gemäß geltendem Recht, je nachdem, was später eintritt.

5. BENENNUNG VON GESCHÜTZTEM MATERIAL

5.1 Vorsicht und Sorgfalt bei der Benennung von zu schützendem Material. Jede Partei oder Nichtpartei, die Informationen oder Gegenstände für den Schutz im Rahmen dieser Anordnung benennt, muss darauf achten, eine solche Benennung auf bestimmtes Material zu beschränken, das nach den entsprechenden Normen als schützenswert einzustufen ist.

Massen-, unterschiedslose oder routinemäßige Benennungen sind verboten. Benennungen, die sich als eindeutig ungerechtfertigt erweisen oder die zu einem unzulässigen Zweck vorgenommen wurden (z.B. um den Fallentwicklungsprozess unnötig zu behindern oder zu verzögern oder um anderen Parteien unnötige Kosten und Belastungen aufzuerlegen), führen zu Sanktionen gegen die benennende Vertragspartei.

Stellt eine benennende Partei fest, dass Informationen oder Gegenstände, die sie zum Schutz bestimmt hat, überhaupt nicht oder nicht in dem ursprünglich geltend gemachten Schutzniveau schützenswert sind, muss die benennende Partei allen anderen Parteien unverzüglich mitteilen, dass sie die irrtümliche Benennung zurückzieht.

5.2 Form und Zeitpunkt der Benennungen. Sofern in dieser Anordnung nichts anderes vorgesehen ist (siehe z.B. Abschnitt 5.2(a) Absatz 2 unten) oder anderweitig festgelegt oder angeordnet, muss Offenlegungs- oder Beweismaterial, das gemäß dieser Anordnung schützenswert ist, vor der Offenlegung oder Vorlegung des Materials klar als solches gekennzeichnet werden.

Eine Benennung in Übereinstimmung mit dieser Anordnung erfordert:

(a) Für Informationen in dokumentarischer Form (z.B. Papier- oder elektronische Dokumente, jedoch mit Ausnahme von Niederschriften von Aussagen oder anderen Vorverhandlungen oder Gerichtsverfahren), dass die vorlegende Partei auf jedem Dokument, das geschütztes Material enthält, die Bezeichnung "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" anbringt.

Eine Partei oder Nichtpartei, die Originaldokumente oder Materialien zur Einsichtnahme zur Verfügung stellt, braucht diese erst dann zum Schutz zu bestimmen, wenn die inspizierende Partei angegeben hat, welches Material sie kopiert und vorgelegt haben möchte. Während der Überprüfung und vor der Kennzeichnung gelten alle Materialien, die zur Einsichtnahme bereitgestellt werden, als „HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR“. Nachdem die prüfende Partei die Dokumente identifiziert hat, die sie kopiert und vorgelegt haben möchte, muss die vorlegende Partei bestimmen, welche Dokumente oder Teile davon nach dieser Anordnung schützenswert sind. Dann muss die vorlegende Partei, bevor sie die festgelegten Dokumente vorlegt, auf jedem Dokument, das geschütztes Material enthält, die entsprechende Bezeichnung ("VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE") anbringen.

(b) für Zeugenaussagen bei der eidesstattlichen Aussage oder in anderen Vorverhandlungs- oder Gerichtsverfahren, dass die benennende Partei vor Abschluss der Aussage, der Verhandlung oder eines anderen Verfahrens alle geschützten Zeugenaussagen zu Protokoll geben und alle Teile der Zeugenaussage, die als "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" qualifiziert sind, weiter spezifizieren kann. Alternativ kann die benennende Partei innerhalb von 30 Tagen nach Erhalt einer Niederschrift oder Aufzeichnung einer eidesstattlichen Aussage oder eines anderen Vorverfahrens oder Gerichtsverfahrens diese Niederschrift oder Aufzeichnung oder einen Teil davon als "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" kennzeichnen,

indem allen Parteien schriftlich mitgeteilt wird, welche Seiten und Zeilen der Abschrift oder der Aufzeichnung als "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" zu behandeln sind. Alle Abschriften oder Aufzeichnungen von Vernehmungen oder anderen Vorverhandlungen oder Gerichtsverfahren werden 30 Tage lang nach Erhalt der Abschrift oder Aufzeichnung oder bis zum Erhalt einer schriftlichen Benachrichtigung über eine Benennung als "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" behandelt, je nachdem, welches Ereignis zuerst eintritt. Im Falle eines nicht parteigebundenen Zeugen kann die Zeugenaussage von einer Partei, dem nicht parteigebundenen Zeugen oder nach Vereinbarung der Parteien als "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" eingestuft werden.

Transkriptionssseiten, die geschütztes Material enthalten, müssen separat durch den Protokollführer des Gerichts gebunden werden, der am oberen Rand jeder dieser Seiten die Bezeichnung "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" entsprechend den Anweisungen der benennenden Partei anbringen muss. Für den Fall, dass die Aussage als Video aufgezeichnet wird, sind das Original und alle Kopien des Videobandes vom Videotechniker zu kennzeichnen, um darauf hinzuweisen, dass der Inhalt des Videobandes dieser Vereinbarten Schutzanordnung unterliegt, im Wesentlichen nach folgendem Muster: "Dieses Videoband enthält vertrauliche Zeugenaussagen, die in diesem Prozess verwendet wurden, und darf nur gemäß den Bestimmungen der wirksamen Vereinbarten Schutzanordnung in dieser Angelegenheit oder gemäß der schriftlichen Vereinbarung der Parteien eingesehen oder deren Inhalt angezeigt oder offengelegt werden.“

Die Parteien benachrichtigen die anderen Parteien, wenn sie angemessenerweise erwarten, dass eine Aussage, Anhörung oder sonstige Vorgänge geschütztes Material beinhalten, so dass die anderen Parteien sicherstellen können, dass nur autorisierte Personen, die das "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben, bei diesen Vorgängen anwesend sind. Die Verwendung eines Dokuments als Beweisstück bei einer Aussage berührt in keiner Weise seine Bezeichnung als "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE".

(c) bei digitalen Dateien und Dokumenten, die in nativem elektronischen Format erstellt wurden, dass die benennende Partei den Dateinamen oder Kennungen Informationen beifügt, aus denen hervorgeht, ob die Datei "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" ist

Material oder eine andere angemessene Methode zur Benennung des geschützten Materials, das in nativem elektronischen Format produziert wurde, zu verwenden. Werden digitale Dateien oder Dokumente, die in einem nativen elektronischen Format erstellt wurden, zur Verwendung bei der Hinterlegung, einem Gerichtsverfahren, einer gerichtlichen Einreichung oder zur Bereitstellung an einen Sachverständigen ausgedruckt, so bringt die Vertragspartei, die die elektronischen Dateien oder Dokumente ausdruckt, auf der ausgedruckten Datei oder dem ausgedruckten Dokument eine Anmerkung an, die der entsprechenden Bezeichnung entspricht und die mit der nativen Datei verbundene Nummer und Bezeichnung der Datei enthält.

(d) für Informationen, die in irgendeiner anderen Form als dokumentarisch erstellt wurden, und für alle anderen materiellen Gegenstände, dass die vorlegende Partei an einer gut sichtbaren Stelle an der Außenseite des Behältnisses oder der Behältnisse, in dem/denen die Informationen oder Gegenstände aufbewahrt werden, den Vermerk "VERTRAULICH", "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" anbringt. Wenn nur ein Teil oder Teile der Informationen oder des Gegenstandes schützenswert sind, identifiziert die vorlegende Partei, soweit durchführbar, den/die zu schützenden Teil/e und gibt den geltend zu machenden Sicherheitsgrad an.

5.3 Unbeabsichtigte Versäumnisse bei der Benennung. Wenn eine unbeabsichtigte Unterlassung, Informationen als qualifizierte Informationen zu kennzeichnen, rechtzeitig korrigiert wird, bedeutet eine unbeabsichtigte Unterlassung, qualifizierte Informationen oder Gegenstände zu benennen, allein noch keinen Verzicht der benennenden Partei auf das Recht, für dieses Material den Schutz gemäß dieser Anordnung sicherzustellen. Bei rechtzeitiger Korrektur einer Benennung muss die empfangende Partei angemessene Anstrengungen unternehmen, um sicherzustellen, dass das Material in Übereinstimmung mit den Bestimmungen dieser Anordnung behandelt wird.

6. ANFECHTEN VON VERTRAULICHEN BENENNUNGEN

6.1 Zeitpunkt für Anfechtungen. Jede Vertragspartei oder Nichtvertragspartei kann die Einstufung der Vertraulichkeit jederzeit anfechten. Eine Vertragspartei verzichtet nicht auf ihr Recht, eine Vertraulichkeitsbenennung anzufechten, indem sie sich dafür entscheidet, keine Anfechtung unverzüglich nach Bekanntgabe der ursprünglichen Benennung vorzunehmen.

6.2 Sitzung und Beratung. Die anfechtende Vertragspartei leitet das Streitbeilegungsverfahren ein, indem sie jede Benennung, die sie anfechtet, schriftlich bekannt gibt und die Grundlage für jede Anfechtung darlegt. Um Unklarheiten darüber zu vermeiden, ob eine Anfechtung erfolgt ist, muss in der schriftlichen Mitteilung darauf hingewiesen werden, dass die Anfechtung der Vertraulichkeit in Übereinstimmung mit diesem

speziellen Absatz der Schutzanordnung erfolgt. Die Parteien versuchen, jede Anfechtung nach Treu und Glauben zu lösen, und müssen den Prozess mit einer direkten Beratung (in einem Dialog von Stimme zu Stimme; andere Formen der Kommunikation sind nicht angemessen) innerhalb von 14 Tagen nach dem Datum der Zustellung der Mitteilung beginnen. Während der Aussprache muss die anfechtende Partei die Grundlage für ihre Annahme erklären, dass die Benennung der Vertraulichkeit nicht angemessen war, und muss der benennenden Partei Gelegenheit geben, das benannte Material zu überprüfen, die Umstände zu überdenken und, falls keine Änderung der Benennung angeboten wird, die Grundlage für die gewählte Benennung zu erläutern. Eine anfechtende Vertragspartei kann nur dann zur nächsten Stufe des Anfechtungsverfahrens übergehen, wenn sie sich zuvor an diesem Sitzungs- und Beratungsverfahren beteiligt hat oder feststellt, dass die benennende Vertragspartei nicht bereit ist, rechtzeitig an dem Sitzungs- und Beratungsverfahren teilzunehmen.

6.3 Gerichtliche Intervention. Wenn die Parteien eine Anfechtung nicht ohne gerichtliche Intervention lösen können, stellt die benennende Partei innerhalb von 14 Tagen, nachdem die Parteien vereinbart haben, dass der Prozess der Sitzung und Beratung ihre Streitigkeit nicht lösen wird, einen Antrag auf Wahrung der Vertraulichkeit nach der lokalen Zivilprozessregel 7 (und gegebenenfalls in Übereinstimmung mit der lokalen Zivilprozessregel 79-5). Jedem derartigen Antrag muss eine Erklärung der zuständigen Behörde beigelegt werden, in der bestätigt wird, dass der Antragsteller die im vorstehenden Absatz aufgestellten Anforderungen für die Sitzung und Beratung erfüllt hat. Unterlässt es die benennende Partei, einen solchen Antrag einschließlich der erforderlichen Erklärung innerhalb der geltenden Frist zu stellen, so verzichtet sie automatisch auf die Vertraulichkeitsbenennung für jede angefochtene Benennung. Darüber hinaus kann die anfechtende Vertragspartei jederzeit einen Antrag auf Anfechtung einer Vertraulichkeitsbenennung stellen, wenn es dafür einen triftigen Grund gibt, einschließlich der Anfechtung der Benennung der Niederschrift einer Aussage oder von Teilen davon. Jedem nach dieser Bestimmung gestellten Antrag muss eine Erklärung der zuständigen Behörde beigelegt werden, in der bestätigt wird, dass der Antragsteller die im vorstehenden Absatz genannten Anforderungen erfüllt und übermittelt hat.

Die Beweislast in einem solchen Anfechtungsverfahren liegt bei der benennenden Vertragspartei. Leichtfertige Anfechtungen und solche, die zu einem unzulässigen Zweck erfolgen (z.B. um andere Parteien zu stören oder ihnen unnötige Kosten und Belastungen aufzuerlegen), können zu Sanktionen gegen die anfechtende Vertragspartei führen. Sofern die benennende Partei nicht auf die Vertraulichkeitsbenennung verzichtet hat, indem sie es versäumt hat, einen Antrag auf Wahrung der Vertraulichkeit wie oben beschrieben einzureichen, gewähren alle Parteien dem

betreffenden Material weiterhin den Schutzzumfang, auf den sie nach der Benennung der erzeugenden Partei Anspruch haben, bis das Gericht über die Anfechtung entscheidet.

7. ZUGANG ZU UND NUTZUNG VON GESCHÜTZTEM MATERIAL

7.1 Grundprinzipien. Eine empfangende Partei darf geschütztes Material, das von einer anderen Partei oder von einer Nichtpartei im Zusammenhang mit diesem Fall offenbart oder vorgelegt wird, nur zur Verfolgung, Verteidigung oder zum Versuch der Beilegung dieses Rechtsstreits verwenden. Eine empfangende Partei darf Geschütztes Material nicht für andere Zwecke verwenden, einschließlich, aber nicht beschränkt auf die Vorbereitung oder Verfolgung von Patenten und Patentanmeldungen, die Anfechtung eines Patents vor einer inländischen oder ausländischen Behörde (einschließlich, aber nicht beschränkt auf einen Wiederausgabeprotest, eine ex-parte-Wiederaufnahmeprüfung oder ein inter-partes-Überprüfungsverfahren) oder in Verbindung mit einem anderen Rechtsstreit oder behördlichen Verfahren. Dieses geschützte Material darf nur den in dieser Anordnung beschriebenen Personengruppen und unter den in dieser Anordnung beschriebenen Bedingungen offenbart werden. Wenn der Rechtsstreit beendet ist, muss eine empfangende Partei die Bestimmungen des nachstehenden Abschnitts 14 (ENDGÜLTIGE OFFENLEGUNG) einhalten.

Geschütztes Material muss von einer empfangenden Partei bei einem Dienstleister in den Vereinigten Staaten und auf eine sichere Art und Weise aufbewahrt und gepflegt werden, die sicherstellt, dass der Zugriff auf die Personen beschränkt ist, die gemäß dieser vereinbarten Schutzanordnung befugt sind. Geschütztes Material kann außerhalb der Vereinigten Staaten eingesehen und überprüft werden.

7.2 Offenlegung von "VERTRAULICHEN" Informationen oder Gegenständen. Sofern nicht anderweitig vom Gericht angeordnet oder von der benennenden Partei schriftlich genehmigt, darf eine empfangende Partei Informationen oder Gegenstände, die als "VERTRAULICH" bezeichnet werden, nur an folgende Personen weitergeben:

(a) den externen Syndikus des Protokolls der empfangenden Partei in diesem Rechtsstreit sowie an die Mitarbeiter des besagten externen Syndikus des Protokolls, an die es vertretbarerweise notwendig ist, die Informationen für diesen Rechtsstreit offenzulegen;

(b) die leitenden Angestellten, Direktoren und Mitarbeiter (einschließlich des Syndikus des Hauses) der empfangenden Partei, denen gegenüber die Offenlegung für diesen Rechtsstreit vernünftigerweise notwendig ist und die die "Anerkennung und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben;

(c) die leitenden Angestellten, Direktoren und Mitarbeiter (einschließlich des Syndikus des Hauses) der empfangenden Partei, denen gegenüber die Offenlegung für diesen Rechtsstreit vertretbarerweise notwendig ist und die die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben;

(d) das Gericht und sein Personal;

(e) Gerichtsreporter oder Kameramänner, die für die Aufzeichnung von Zeugenaussagen in diesem Verfahren herangezogen wurden, und ihre jeweiligen Mitarbeiter;

(f) Professionelle Geschworene oder Prozessberater, Scheingeschworene und professionelle Dienstleister, denen die Offenlegung für diesen Rechtsstreit vertretbarerweise notwendig ist und die die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben;

(g) während ihrer Aussagen, Zeugen in der Klage, denen gegenüber eine Offenlegung vertretbarerweise notwendig ist, es sei denn, die benennende Partei hat etwas anderes vereinbart oder vom Gericht angeordnet. Seiten von transkribierten Zeugenaussagen oder Exponaten zu Zeugenaussagen, die geschütztes Material enthüllen, müssen separat vom Gerichtsreporter gebunden werden und dürfen niemandem offengelegt werden, es sei denn, dies ist im Rahmen dieser vereinbarten Schutzanordnung gestattet.

(h) jeder einvernehmlich vereinbarte Vermittler oder Vergleichsbeamte und sein unterstützendes Personal;

(i) der Autor oder Empfänger eines Dokuments, das die Informationen enthält, oder ein Vormund oder eine andere Person, die die Informationen anderweitig besaß oder kannte; und

(j) jede andere Person auf gerichtliche Anordnung oder nach vorheriger schriftlicher Zustimmung der benennenden Partei.

7.3 Offenlegung von als "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" und "HOCH VERTRAULICH - QUELLCODE" deklarierten Informationen oder Gegenständen. Sofern nicht anderweitig vom Gericht angeordnet oder von der benennenden Partei schriftlich genehmigt, darf eine empfangende Partei Informationen oder Gegenstände, die als "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" bezeichnet werden, nur an folgende Personen weitergeben:

(a) den externen Syndikus des Protokolls der empfangenden Partei in diesem Rechtsstreit sowie an die Mitarbeiter des besagten externen Syndikus des Protokolls, an die es vertretbarerweise notwendig ist, die Informationen für diesen Rechtsstreit offenzulegen;

(a) den benannten Syndikus des Hauses der empfangenden Partei, (i) an den die Offenlegung für diesen Rechtsstreit vertretbarerweise notwendig ist, (ii) der die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet hat, und (iii) der die in Absatz 7.4(a)-(c) unten dargelegten Verfahren befolgt hat;¹

(b) Experten der empfangenden Partei (1) denen die Offenlegung für diesen Rechtsstreit vertretbarerweise vonnöten ist, (2) die die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben, und (3) welche die in Absatz 7.4(a)-(c) unten dargelegten Verfahren befolgt haben;

(c) das Gericht und sein Personal;

(d) Gerichtsreporter oder Kameramänner, die für die Aufzeichnung von Zeugenaussagen in diesem Verfahren herangezogen wurden, und ihre jeweiligen Mitarbeiter,

(e) professionelle Geschworene oder Prozessberater, Scheingeschworene und professionelle Dienstleister, denen die Offenlegung für diesen Rechtsstreit vertretbarerweise notwendig ist und die die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben; "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A)

(f) der Autor oder Empfänger eines Dokuments, das die Informationen enthält, oder ein Vormund oder eine andere Person, die die Informationen anderweitig besaß oder kannte; und

(g) jede andere Person auf gerichtliche Anordnung oder nach vorheriger schriftlicher Zustimmung der benennenden Partei.

7.4 Verfahren für die Genehmigung oder den Einspruch gegen die Offenlegung von Informationen oder Gegenständen, die "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" sind, gegenüber dem benannten Syndikus des Hauses oder Experten.

Sofern nicht anderweitig vom Gericht angeordnet oder von der benennenden Partei schriftlich genehmigt, muss eine empfangende Partei, die dem benannten Syndikus des Hauses oder einem Experten (wie in dieser Anordnung bestimmt) jegliche Informationen oder Gegenstände, die als "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELL

¹ Diese Anordnung bestimmt, dass benannte Syndizi des Hauses keinen Zugriff auf Informationen oder Gegenstände mit der Bezeichnung "HOCH VERTRAULICH - QUELLCODE" haben, mit Ausnahme des Quellcodes, der in Expertengutachten und Gerichtsakten enthalten ist.

CODE" bezeichnet werden, gemäß Absatz 7. 3(c) zuerst einen schriftlichen Antrag an die benennende Partei stellen, in dem (1) die allgemeinen Kategorien von Informationen mit der Bezeichnung "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" angegeben werden, für die die empfangende Partei um die Erlaubnis bittet, sie an den benannten Syndikus des Hauses oder einem Experten weiterzugeben, (2) den vollständigen Namen des benannten Syndikus des Hauses oder des Experten sowie die Stadt und den Staat seines Hauptwohnsitzes angibt, (3) für einen Experten eine Kopie seines aktuellen Lebenslaufs beifügt, (4) für einen Experten den/die aktuellen Arbeitgeber des Experten angibt, (5) für einen Experten jede Person oder Organisation angibt, von der der Experte zu irgendeinem Zeitpunkt während der vorangegangenen fünf Jahre eine Vergütung oder Finanzierung für die Arbeit in seinen Fachgebieten erhalten hat oder für die der Experte zu irgendeinem Zeitpunkt während der vorangegangenen fünf Jahre professionelle Dienstleistungen, auch in Verbindung mit einem Rechtsstreit, erbracht hat, 2 und (6) für einen Experten (mit Namen und Nummer des Falles, Verhandlungsdatum und Ort des Gerichts) jeden Rechtsstreit angibt, für den der Experte während der vorangegangenen fünf Jahre eine Expertenaussage, auch durch eine Erklärung, einen Bericht oder eine Zeugenaussage bei einer eidesstattlichen Aussage oder Verhandlung, geleistet hat.

(a) Eine Partei, die einen Antrag stellt und die in Absatz (a) genannten Informationen zur Verfügung stellt, kann das geschützte Material dem benannten Syndikus des Hauses oder Experten offenlegen, es sei denn, die Partei erhält innerhalb von 14 Tagen nach Zustellung des Antrags einen schriftlichen Einspruch von der benennenden Partei. Ein solcher Einspruch muss die Gründe, auf die er sich stützt, im Einzelnen darlegen.

(b) Eine Partei, die rechtzeitig einen schriftlichen Einspruch nach Absatz (b) erhält, muss mit der benennenden Partei konferieren (durch direkten Dialog von Angesicht zu Angesicht), um zu versuchen, die Angelegenheit innerhalb von sieben Tagen nach dem schriftlichen Einspruch einvernehmlich zu lösen. Kommt keine Einigung zustande, kann die Partei, die die Offenlegung gegenüber dem Rechtsbeistand oder Sachverständigen der designierten Kammer anstrebt, einen Antrag gemäß der lokalen Zivilprozessregel 7 (und gemäß der lokalen Zivilprozessregel 79-5, falls anwendbar) stellen und das Gericht um die Erlaubnis bitten, dies zu tun. Ein solcher Antrag muss die Umstände spezifisch beschreiben, detailliert die Gründe darlegen, warum die Offenlegung gegenüber dem benannten

² Ist der Experte der Ansicht, dass eine dieser Informationen einer Geheimhaltungspflicht gegenüber Dritten unterliegt, so sollte der Experte alle Informationen zur Verfügung stellen, von denen er glaubt, dass sie ohne Verletzung von Geheimhaltungsvereinbarungen offengelegt werden können, und die Partei, die die Offenlegung gegenüber dem Experten anstrebt, ist für ein Treffen mit der benennenden Partei verfügbar und berät sich mit ihr über eine derartige Vereinbarung.

Syndikus des Hauses oder Experten vertretbarerweise notwendig ist, das Schadensrisiko abschätzen, das die Offenlegung mit sich bringen würde, und alle zusätzlichen Mittel vorschlagen, die zur Verringerung dieses Risikos eingesetzt werden könnten. Darüber hinaus muss jedem derartigen Antrag eine Erklärung der zuständigen Stelle beigefügt werden, in der die Bemühungen der Parteien um eine einvernehmliche Lösung der Angelegenheit (d.h. Umfang und Inhalt der Zusammenkünfte und Beratungen) beschrieben und die von der benennenden Partei vorgebrachten Gründe für ihre Ablehnung der Genehmigung der Offenlegung dargelegt werden.

In einem solchen Verfahren trägt die Partei, die sich der Offenlegung gegenüber dem benannten Syndikus des Hauses oder Experten verwehrt, die Beweislast dafür, dass das Risiko eines Schadens, den die Offenlegung (unter den vorgeschlagenen Schutzmaßnahmen) mit sich bringen würde, die Notwendigkeit der empfangenden Partei überwiegt, das geschützte Material gegenüber ihrem benannten Syndikus des Hauses oder Experten offenzulegen.

7.5 Offenlegung von Aussagen gemäß California _Civil _Code Abschnitt 2019.210. Ungeachtet anderer Bestimmungen dieser Schutzanordnung können die Angeklagten vier nicht anwaltliche Mitarbeiter der Angeklagten bestimmen, die zur Unterstützung der Verteidigung der Behauptungen von Teradata über den entsprechenden technischen und produktbezogenen Hintergrund verfügen und die die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) unterzeichnet haben, Folgendes offen legen: "Plaintiffs Teradata Corporation, Teradata US, Inc., und Teradata Operations, Inc.'s Liste der geltend gemachten Geschäftsgeheimnisse gemäß California Civil Code Abschnitt 2019.210", die am 21. Dezember 2018 versandt wurde, jede spätere Offenlegung durch die Kläger gemäß Abschnitt 2019.210 sowie alle Dokumente oder Texte, auf die in der Liste nach Abschnitt 2019.210 ausdrücklich Bezug genommen wird, einschließlich der Orange Books von Teradata. Die Angeklagten müssen jeden dieser nicht anwaltlichen Mitarbeiter den Klägern mindestens 14 Tage vor der Offenlegung gegenüber diesem Mitarbeiter identifizieren, und wenn die Kläger Einspruch erheben, gilt das in Abschnitt 7.4 dieser Schutzanordnung festgelegte Verfahren; vorausgesetzt jedoch, dass die Beteiligung des Mitarbeiters an der Entwicklung von Produkten, die nach Ansicht von Teradata Konkurrenzprodukte sind, an sich kein Grund für einen Einspruch ist. Sollten die Angeklagten anschließend der Ansicht sein, dass eine Offenlegung gegenüber weiteren Mitarbeitern, die keine Anwälte sind, gerechtfertigt ist, werden beide Seiten in gutem Glauben die Hinzufügung einer verhältnismäßigen und angemessenen Anzahl weiterer Mitarbeiter, die keine Anwälte sind, erörtern. In dem Maße, in dem keine Übereinkunft erzielt werden kann, werden die Parteien das Gericht um Rat fragen.

8. QUELLCODE

(a) Eine Produzierende Partei kann Quellcode als "HOCH VERTRAULICH - QUELLCODE" für alle in Absatz 2.9 genannten Informationen oder Gegenstände kennzeichnen, wenn sie einen vertraulichen, urheberrechtlich geschützten oder als Geschäftsgeheimnis eingestuften Quellcode enthalten oder einschließen.

(b) Geschütztes Material, das als "HOCH VERTRAULICH - QUELLCODE" gekennzeichnet ist, unterliegt allen Schutzmaßnahmen, die für "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBARE" Informationen gewährt werden, und darf nur an die Personen weitergegeben werden, an die "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBARE" Informationen weitergegeben werden dürfen, wie in den Absätzen 7.3 und 7.4 dargelegt.

(c) Geschütztes Material mit der Bezeichnung "HOCH VERTRAULICH - QUELLCODE" wird zur Einsichtnahme während der normalen Geschäftszeiten oder zu anderen einvernehmlich vereinbarten Zeiten in zwei Büros des Anwalts der Produzierenden Partei oder an anderen einvernehmlich vereinbarten Orten in einem Format zur Verfügung gestellt, das eine angemessene Überprüfung und Durchsicht ermöglicht. Derartiges Material wird zur Einsichtnahme in einem gesicherten Raum auf einem gesicherten Computer ohne Internetzugang oder Netzwerkzugang zu anderen Computern zur Verfügung gestellt, und die empfangende Partei darf keinen Teil des Quellcodes auf ein beschreibbares Medium oder ein beschreibbares Gerät kopieren, entfernen oder anderweitig übertragen. Die produzierende Partei darf die Aktivitäten der Vertreter der empfangenden Partei während einer Überprüfung des HOCH VERTRAULICHEN - QUELLCODES visuell überwachen, jedoch nur, um sicherzustellen, dass die als HOCH VERTRAULICHEN - QUELLCODE bezeichneten Informationen nicht unbefugt aufgezeichnet, kopiert oder übertragen werden.³

(d) Die empfangende Partei kann Papierkopien begrenzter Teile des Quellcodes anfordern, die in diesem Verfahren vertretbarerweise für die Anfertigung von Gerichtsakten, Schriftsätzen, Expertengutachten oder anderen Papieren oder für die Aussage oder Verhandlung erforderlich sind, darf jedoch keine Papierkopien zum Zwecke der Überprüfung des Quellcodes anfordern, es sei denn in elektronischer Form, wie in Absatz (c) in erster Instanz festgelegt.

³ Unter bestimmten Umständen kann es zweckdienlich sein, von der empfangenden Partei zu verlangen, ein Protokoll in Papierform zu führen, in dem die Namen aller Personen, die die Informationen des HOCH VERTRAULICHEN - QUELLCODES einsehen, sowie Datum und Uhrzeit der Einsichtnahme und die Namen aller Personen angegeben werden, denen Papierkopien von Teilen des Quellcodes zur Verfügung gestellt werden.

Die vorlegende Partei kann die Menge des in Papierform angeforderten Quellcodes gemäß dem in Absatz 6 festgelegten Schlichtungsverfahren und Zeitrahmen anfechten, wobei die vorlegende Partei die "anfechtende Partei" und die empfangende Partei die "benennende Partei" für die Schlichtung von Streitigkeiten darstellt. Die erzeugende Partei druckt den ausgewiesenen Quellcode auf gelbes (oder anderes nicht weißes) farbiges Papier. Die produzierende Partei kennzeichnet jede Seite deutlich mit Bates-Nummern und dem Vermerk " HOCH VERTRAULICH - QUELLCODE."

(e)Die empfangende Partei führt Aufzeichnungen über jede Person, die einen Teil des Quellcodes in elektronischer oder Papierform eingesehen hat. Die empfangende Partei bewahrt alle Papierkopien aller gedruckten Teile des Quellcodes an einem sicheren, verschlossenen Ort auf. Die empfangende Partei darf keine elektronischen oder sonstigen Abbilder der Papierkopien erstellen und die Papierkopien nicht in ein elektronisches Format umwandeln. Die empfangende Partei kann die Erlaubnis erhalten, kurze Auszüge des Quellcodes (20 Zeilen oder weniger) in Gerichtsakten oder Expertengutachten aufzunehmen, solange diese Dokumente als "HOCH VERTRAULICH - QUELLCODE" deklariert sind. Die empfangende Partei darf nur dann zusätzliche Papierkopien anfertigen, wenn diese zusätzlichen Kopien (1) zur Anfertigung von Gerichtsakten, Schriftsätzen oder anderen Schriftstücken (einschließlich eines Gutachtens eines aussagenden Experten), (2) für die Aussage erforderlich sind oder (3) anderweitig für die Vorbereitung des Falles notwendig sind. Alle Papierkopien, die während einer Aussage verwendet werden, sind von der vorlegenden Partei am Ende eines jeden Tages abzurufen und dürfen nicht an einen Gerichtsreporter oder eine andere nicht befugte Person ausgehändigt oder bei dieser gelassen werden. 4 Die empfangende Partei kann verlangen, dass die herstellende Partei einen Quellcode Computer zu einer Hinterlegung mitbringt; die vorlegende Partei muss dieser Forderung nachkommen, es sei denn, ihre Einhaltung wäre mit einer unangemessenen Belastung verbunden.

9. GESCHÜTZTES MATERIAL, DAS IN EINEM ANDEREN RECHTSSTREIT VORGELEGT ODER VORGELEGT WERDEN SOLL

Wenn einer Partei eine in einem anderen Rechtsstreit erlassene Vorladung oder ein Gerichtsbeschluss zugestellt wird, der die Offenlegung von Informationen oder Gegenständen erzwingt, die in dieser Klage als "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" eingestuft sind, muss diese Partei:

4 Die Beschaffenheit der als "HOCH VERTRAULICH - QUELLCODE" ausgewiesenen Informationen, um die es in einem bestimmten Fall geht, kann zusätzliche Schutzvorkehrungen oder Einschränkungen rechtfertigen. Beispielsweise kann es unter bestimmten Umständen angemessen sein, von der empfangenden Partei zu verlangen, dass sie die vorlegende Partei benachrichtigt, bevor sie Informationen, die als " HOCH VERTRAULICH - QUELLCODE" ausgewiesen sind, in einen Gerichtsantrag, einen Schriftsatz oder einen Expertenbericht aufnimmt.

(a) die benennende Partei unverzüglich schriftlich benachrichtigen. Diese Mitteilung muss eine Kopie der Vorladung oder des Gerichtsbeschlusses enthalten;

(b) der Partei, die die Vorladung oder Anordnung in dem anderen Rechtsstreit veranlasst hat, unverzüglich schriftlich mitteilen, dass das gesamte oder ein Teil des Materials, das Gegenstand der Vorladung oder Anordnung ist, dieser Schutzanordnung unterliegt. Eine solche Benachrichtigung muss eine Kopie dieser vereinbarten Schutzanordnung enthalten; und

(c) in Bezug auf alle vertretbaren Verfahren kooperieren, die von der benennenden Partei, deren geschütztes Material betroffen sein könnte, angestrebt werden.⁵

Wenn die benennende Partei rechtzeitig eine Schutzanordnung beantragt, darf die Partei, der die Vorladung oder gerichtliche Anordnung zugestellt wurde, keine Informationen, die in dieser Klage als "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" eingestuft sind, vor einer Entscheidung des Gerichts, von dem die Vorladung oder Anordnung erlassen wurde, vorlegen, es sei denn, die Partei hat die Zustimmung der benennenden Partei eingeholt. Die benennende Partei trägt die Last und die Kosten, die damit verbunden sind, vor diesem Gericht den Schutz ihres vertraulichen Materials zu beantragen - und nichts in diesen Vereinbarungen sollte dahingehend ausgelegt werden, dass es eine empfangende Partei in dieser Klage ermächtigt oder ermutigt, eine rechtmäßige Anordnung eines anderen Gerichts zu missachten.

10. GESCHÜTZTES MATERIAL EINER NICHTPARTEI, DAS IN DIESEM RECHTSSTREIT VORGELEGT WERDEN SOLL

(a) Die Bedingungen dieser Anordnung gelten für Informationen, die von einer Nichtpartei im Rahmen dieser Klage erstellt wurden und als "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" deklariert sind. Solche Informationen, die von Nichtparteien im Zusammenhang mit diesem Rechtsstreit vorgelegt werden, sind durch die Rechtsmittel und Rechtsbehelfe geschützt, die in dieser vereinbarten Schutzanordnung festgelegt sind.

⁵ Der Zweck der Auferlegung dieser Pflichten besteht darin, die betroffenen Parteien auf die Existenz dieser Schutzanordnung aufmerksam zu machen und der benennenden Partei in diesem Fall Gelegenheit zu geben, zu versuchen, ihre Geheimhaltungsinteressen vor dem Gericht, von dem die Vorladung oder Anordnung erlassen wurde, zu schützen.

Nichts in dieser Anordnung sollte so ausgelegt werden, dass es einer Nichtpartei untersagt ist, zusätzliche Schutzmaßnahmen zu beantragen.

(b) Für den Fall, dass eine Partei durch einen gültigen Offenlegungsantrag aufgefordert wird, die in ihrem Besitz befindlichen vertraulichen Informationen einer Nichtpartei vorzulegen, und die Partei einer Vereinbarung mit der Nichtpartei unterliegt, die vertraulichen Informationen der Nichtpartei nicht vorzulegen, so ist die Partei verpflichtet:

1. die ersuchende Partei und die Nichtpartei unverzüglich schriftlich davon in Kenntnis zu setzen, dass einige oder alle der angeforderten Informationen einer Verschwiegenheitsvereinbarung mit einer Nichtpartei unterliegen;
2. der Nichtpartei umgehend eine Kopie der vereinbarten Schutzanordnung in diesem Rechtsstreit, den/die entsprechenden Offenlegungsantrag/Anträge und eine hinreichend genaue Beschreibung der angeforderten Informationen zukommen zu lassen; und
3. die angeforderten Informationen zur Begutachtung durch die Nichtpartei zur Verfügung zu stellen.

(c) Wenn die Nichtpartei nicht innerhalb von 14 Tagen nach Erhalt der Mitteilung und der dazugehörenden Informationen bei diesem Gericht Einspruch erhebt oder eine Schutzanordnung beantragt, kann die empfangende Partei die vertraulichen Informationen der Nichtpartei als Antwort auf den Antrag auf Offenlegung vorlegen. Wenn die Nichtpartei rechtzeitig eine Schutzanordnung beantragt, darf die empfangende Partei keine in ihrem Besitz oder unter ihrer Kontrolle befindlichen Informationen, die der Verschwiegenheitsvereinbarung mit der Nichtpartei unterliegen, vor einer Entscheidung des Gerichts vorlegen. Sofern kein gegenteiliger Gerichtsbeschluss vorliegt, trägt die Nichtpartei die Last und die Kosten für die Beantragung des Schutzes ihres geschützten Materials vor diesem Gericht.

11. NICHT AUTORISIERTE OFFENLEGUNG VON GESCHÜTZTEM MATERIAL

Wenn eine empfangende Partei erfährt, dass sie durch ein Versehen oder auf andere Weise geschütztes Material an eine andere Person oder unter anderen Umständen offenbart hat, die nach dieser Verordnung nicht autorisiert sind, muss die empfangende Partei unverzüglich (a) die benennende Partei schriftlich über die nicht autorisierten Offenlegungen informieren, (b) sich nach besten Kräften bemühen, alle unautorisierten Kopien des geschützten Materials sicherzustellen, (c) die Person(en), der/denen unautorisierte Offenlegungen gemacht wurden, über alle Bedingungen dieser Anordnung informieren und (d) diese Person(en) auffordern, die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" (Anhang A) zu unterzeichnen.

Unautorisierte oder versehentliche Offenlegung ändert weder den Status von geschütztem Material, noch verzichtet sie auf das Recht, das offengelegte Dokument oder die offengelegte Information als geschütztes Material zu erhalten.

12. VORLEGUNG VON VERTRAULICHEM ODER ANDERWEITIG GESCHÜTZTEM MATERIAL

Keine Bestimmung in dieser vereinbarten Schutzanordnung verlangt die Offenlegung von Informationen, die durch das Anwaltsgeheimnis, die Immunität von Arbeitsleistungen oder andere Privilegien oder Immunitäten geschützt sind. Die Vorlegung von vertraulichen oder durch das Arbeitsergebnis geschützten Dokumenten, elektronisch gespeicherten Informationen ("ESI") oder Informationen stellt in diesem Fall oder in einem anderen Verfahren auf Bundes- oder Landesebene keinen Verzicht auf das Recht oder den Schutz vor Offenlegung dar, es sei denn, die vorlegende Partei teilt mit, dass sie absichtlich und wissentlich auf ein Recht oder eine Immunität verzichtet, dann wird dieses Recht oder diese Immunität in diesem Fall aufgehoben. Diese Anordnung ist so auszulegen, dass sie den nach der Federal Rule of Evidence 502(d) erlaubten maximalen Schutz bietet. Zur Vermeidung von Zweifeln und für die Anwendung dieses Absatzes vereinbaren die Parteien, dass die Federal Rule of Evidence 502(b) nicht anwendbar ist.

Zur Gewährleistung einer gerechten, zügigen und kostengünstigen Entscheidung über diese Klage nach der Federal Rule of Civil Procedure 1 vereinbaren die Parteien, sich nach besten Bemühungen um die Einhaltung des folgenden Grundsatzes zu bemühen: Wenn eine empfangende Partei bei der Durchsicht des ihr vorgelegten Offenlegungs- oder Beweismaterials feststellt, dass irgendein Teil dieses Offenlegungs- oder Beweismaterials durch das Anwaltsgeheimnis, die Immunität für das Arbeitsergebnis oder ein anderes Privileg oder eine andere Immunität geschützt ist, hat die empfangende Partei die produzierende Partei unverzüglich über die spezifischen Materialien zu informieren, die in Betracht gezogen werden könnten, und wird diese Materialien nicht für irgendwelche Zwecke verwenden, bis die Frage durch Übereinkunft der Parteien oder durch Beschluss des Gerichts geklärt ist. Die unbeabsichtigte Nichteinhaltung dieses Grundsatzes begründet keinen Anspruch auf Entlastung.

Wenn eine produzierende Partei einer empfangenden Partei mitteilt, dass bestimmtes versehentlich vorgelegtes Offenlegungs- oder Beweismaterial einem Anspruch auf ein Sonderrecht oder sonstigen Schutz unterliegt, sind die Verpflichtungen der empfangenden Partei diejenigen, die in der Federal Rule of Civil Procedure 26(b)(5)(B) festgelegt sind. Jede empfangende Partei muss dieses Offenlegungs- oder Beweismaterial und alle Kopien unverzüglich an die produzierende Partei zurückgeben, mit Ausnahme von Seiten, die vertrauliche Kennzeichnungen der empfangenden Partei enthalten, die stattdessen vernichtet und als solche von der empfangenden Partei gegenüber der produzierenden Partei anerkannt werden.

Nichts, was in diesem Dokument festgelegt ist, hat die Absicht oder soll dazu dienen, das Recht einer Partei zu beschränken, eine Überprüfung von Dokumenten, ESI oder Informationen (einschließlich Metadaten) auf Relevanz, Aktualität und/oder die Trennung von privilegierten und/oder geschützten Informationen vor der Vorlegung zu veranlassen. Diese Regelung soll nicht dazu dienen, jegliches in einer E-Discovery-Anordnung festgelegtes Verfahren zu ändern, das eine Vorlegung ohne vorherige Überprüfung der Vertraulichkeit vorsieht.

13. SONSTIGES

13.1 Recht auf weitere Rechtsmittel. Keine Bestimmung dieser Anordnung schränkt das Recht einer Person ein, in Zukunft ihre Änderung durch das Gericht zu beantragen.

13.2 Recht auf Geltendmachung von sonstigen Einsprüchen. Durch die Vereinbarung der Erlassung dieser Schutzanordnung verzichtet keine Partei auf ein Recht, das sie andernfalls gegen die Offenlegung oder Vorlage von Informationen oder Gegenständen aus Gründen geltend machen müsste, die nicht in dieser festgelegten Schutzanordnung behandelt werden. Gleichmaßen verzichtet keine Partei auf das Recht, aus irgendeinem Grund Einspruch gegen die Verwendung als Beweismittel für die Verwendung des von dieser Schutzanordnung erfassten Materials zu erheben.

13.3 Exportkontrolle. Die Offenlegung von geschütztem Material unterliegt allen anwendbaren Gesetzen und Vorschriften in Bezug auf den Export der in diesem geschützten Material enthaltenen technischen Daten, einschließlich der Weitergabe dieser technischen Daten an ausländische Personen oder Staatsangehörige der Vereinigten Staaten oder anderswo. Die vorlegende Partei ist für die Identifizierung solcher kontrollierten technischen Daten verantwortlich, und die empfangende Partei ergreift die erforderlichen Maßnahmen, um die Einhaltung zu gewährleisten.

13.4 EINREICHUNG VON GESCHÜTZTEM MATERIAL Ohne die schriftliche Genehmigung der benennenden Partei oder einen Gerichtsbeschluss, der nach entsprechender Benachrichtigung aller interessierten Personen erwirkt wurde, darf eine Partei im Rahmen dieses Verfahrens kein geschütztes Material öffentlich einreichen. Eine Partei, die versucht, geschütztes Material unter Verschluss einzureichen, muss die lokale Zivilprozessregel 79-5 einhalten. Geschütztes Material darf nur gemäß einer gerichtlichen Anordnung, die den Verschluss des betreffenden geschützten Materials genehmigt, unter Verschluss eingereicht werden. Gemäß der lokalen Zivilprozessordnung 79-5 wird eine Verschlussverfügung nur auf einen Antrag hin erlassen, in dem festgestellt wird, dass das fragliche geschützte Material vertraulich ist, als Geschäftsgeheimnis schützenswert ist oder anderweitig Anspruch auf Schutz durch das Gesetz hat. Wird der Antrag einer empfangenden Partei, geschütztes Material gemäß der lokalen Zivilprozessordnung 79-5(e) unter Verschluss einzureichen, vom Gericht abgelehnt, so kann die empfangende Partei das geschützte Material gemäß der lokalen Zivilprozessordnung 79-5(e)(2) in das öffentliche Verzeichnis aufnehmen, sofern das Gericht nichts anderes anordnet.

13.5 Berechnung der Frist: Die Berechnung jeglicher Fristen, die durch diese Schutzanordnung vorgeschrieben oder erlaubt sind, unterliegt den Bestimmungen für die Berechnung der Frist in der Federal Rule of Civil Procedure 6, sofern in der lokalen Zivilprozessordnung 7 keine anderen Bestimmungen vorgeschrieben sind.

13.6 Rechtsnachfolger: Diese vereinbarte Schutzanordnung ist für die Parteien, ihren Rechtsbeistand und ihre Nachfolger, Testamentsvollstrecker, Erben, Rechtsnachfolger und Mitarbeiter rechtsverbindlich.

13.7 Benennung unzulässig: Der Umstand der Benennung oder des Versäumnisses, Offenlegungs- oder Beweismaterial als "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" gemäß dieser vereinbarten Schutzanordnung zu benennen, ist zu keinem Zweck in einer Hauptverhandlung oder in einem anderen Prozess als einem solchen, der sich aus dieser vereinbarten Schutzanordnung ergibt oder damit zusammenhängt, zulässig.

14. ENDGÜLTIGE BEILEGUNG

Innerhalb von 60 Tagen nach der endgültigen Beilegung dieser Klage, wie in Absatz 4 definiert, muss jede empfangende Partei alles geschützte Material an die produzierende Partei zurückgeben oder dieses Material vernichten. Im Sinne dieser Definition umfasst "sämtliches geschütztes Material" alle Kopien, Zusammenfassungen, Zusammenstellungen, Auszüge, Kurzfassungen und jedes andere Format, in dem das geschützte Material vervielfältigt oder erfasst wurde. Unabhängig davon, ob das geschützte Material zurückgegeben oder vernichtet wird, muss die empfangende Partei der vorlegenden Partei (und, wenn es sich nicht um dieselbe natürliche oder juristische Person handelt, der benennenden Partei) innerhalb der 60-Tage-Frist eine schriftliche Bescheinigung vorlegen, in der (1) (gegebenenfalls nach Kategorie) das gesamte geschützte Material, das zurückgegeben oder vernichtet wurde, aufgeführt ist und (2) bestätigt wird, dass die empfangende Partei keine Kopien, Zusammenfassungen, Zusammenstellungen, Auszüge oder jedes andere Format, in dem das geschützte Material reproduziert oder erfasst wurde, einbehalten hat. Unabhängig von dieser Bestimmung ist der Syndikus berechtigt, eine Archivkopie aller Plädoyers, Antragsschriften, Prozess-, Hinterlegungs- und Verhandlungsprotokolle, juristischen Memoranden, Korrespondenz, Expertenberichte, Arbeitsunterlagen des Anwalts und Arbeitsunterlagen von Beratern und Experten einzubehalten, auch wenn diese Materialien geschütztes Material enthalten. Sämtliche derartigen Archivkopien, die geschütztes Material enthalten oder geschütztes Material darstellen, unterliegen weiterhin dieser Schutzanordnung, wie in Abschnitt 4 (DAUER) dargelegt.

15. DATENSICHERHEIT

Jede Partei, die im Besitz von Beweismaterial ist, das als "VERTRAULICH" oder "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICH - QUELLCODE" deklariert ist, ist verpflichtet, ein schriftliches Datensicherheitsprogramm bereitzustellen, das angemessene administrative, technische und physische Sicherheitsvorkehrungen zum Schutz der Datensicherheit und Geheimhaltung, zum Schutz vor allen begründeten Bedrohungen oder Gefahren für die Datensicherheit und zum Schutz vor unberechtigtem Zugang zu oder unberechtigter Nutzung dieser Daten gewährleistet. Sollte eine Partei nicht über ein Datensicherheitsprogramm verfügen, kann sie diese Bestimmung erfüllen, indem sie das Beweismaterial mit dem "VERTRAULICHEN" oder "HOCH VERTRAULICHEN - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICHEN - QUELLCODE" von eDiscovery-Anbietern oder Anspruchsverwaltern, die ein solches Datensicherheitsprogramm unterhalten, verwalten und/oder bei diesen speichern lässt. Stellt die empfangende Partei eine Verletzung der Sicherheit fest, einschließlich eines tatsächlichen oder vermuteten unbefugten Zugriffs im Zusammenhang mit dem "VERTRAULICHEN" oder "HOCH VERTRAULICHEN - NUR FÜR ANWÄLTE EINSEHBAR" oder "HOCH VERTRAULICHEN - QUELLCODE" Beweismaterial einer anderen Partei, so ist die empfangende Partei verpflichtet:

(1) die benennende Partei unverzüglich schriftlich von einem solchen Verstoß in Kenntnis zu setzen;

(2) die Auswirkungen des Vertragsbruchs zu untersuchen und angemessene Anstrengungen zu unternehmen, um die Auswirkungen des Vertragsbruchs zu beheben, und der benennenden Partei hinreichend zufriedenstellende Zusicherungen zu geben, dass sich der Vertragsbruch nicht wiederholt;

und (3) ausreichende Informationen über den Vertragsbruch zur Verfügung zu stellen, damit die benennende Partei den Umfang und die Tragweite des Vertragsbruchs in angemessener Weise feststellen kann. Falls ein gerichtliches oder staatliches Ersuchen, eine gerichtliche Auflage oder Anordnung zur Offenlegung solcher Informationen erforderlich ist, unternimmt die empfangende Partei alle angemessenen Schritte, um die benennende Partei rechtzeitig vorher zu benachrichtigen, damit sie dieses Ersuchen, diese Auflage oder Anordnung mit rechtlichen Mitteln anfechten kann. Die empfangende Partei erklärt sich bereit, mit der benennenden Partei oder den Justizbehörden bei der Untersuchung eines solchen sicherheitsrelevanten Vorfalls zusammenzuarbeiten. In jedem Fall ergreift die empfangende Partei unverzüglich alle notwendigen und angemessenen Maßnahmen, um den unberechtigten Zugang zu unterbinden.

SO WIRD ES DURCH DEN SYNDIKUS DER PROTOKOLLS BESCHLOSSEN.

MIT DATUM VOM: 13. Mai 2019

/s/ Mark Whitaker

MORRISON & FOERSTER LLP

Anwälte der Kläger
TERADATA CORP.,
TERADATA US, INC., und
TERADATA OPERATIONS, INC.

MIT DATUM VOM: 13. Mai 2019

/s/ Tharan Gregory Lanier

JONES DAY
PAUL, WEISS, RIFKIND, WHARTON &
GARRISON LLP

Anwälte der Angeklagten
SAP SE,
SAP AMERICA, INC., und
SAP LABS LLC

GEMÄß DEN BESTIMMUNGEN WIRD DIES SO ANGEORDNET.

MIT 14. Mai 2019

[Unterschrift]

DATUM

VOM:

Magistratsrichterin Elizabeth B. LaPorte
Richterin am Amtsgericht der Vereinigten Staaten
Magistrat

BESCHEINIGUNG DER ELEKTRONISCH EINGEREICHTEN UNTERSCHRIFT

Ich, Mark L. Whitaker, bin der ECF-Benutzer, dessen Benutzer-ID und Passwort für die Einreichung dieser vereinbarten geplanten Schutzanordnung verwendet werden. Entsprechend der Lokalen Regel 5-1(i)(3) bestätige ich hiermit, dass die Zustimmung zur Einreichung dieses Dokuments von jedem Unterzeichner dieses Dokuments eingeholt wurde.

Ausgeführt am 13. Mai 2019

/s Mark Whitaker

Mark Whitaker

ANHANG AANERKENNTNIS UND EINVERSTÄNDNIS, VERTRAGLICH GEBUNDEN ZU SEIN

Ich, _____ [vollständiger Name], wohnhaft in _____
[vollständige Adresse], erkläre unter Androhung einer Strafe wegen Meineids, dass ich die vereinbarte Schutzanordnung vollständig gelesen und verstanden habe, die vom United States District Court for the Northern District of California am _____ [Datum] erlassen wurde, im Fall *Teradata Corporation, et al. v. SAP SE, et al.* Fall Nr. 3:18-cv-03670-WHO (N.D. Cal.). Ich erkläre mich damit einverstanden, mich an alle Bestimmungen dieser vereinbarten Schutzanordnung zu halten und an sie gebunden zu sein, und ich verstehe und erkenne an, dass ich mich bei Nichteinhaltung dieser Anordnung Sanktionen und Strafen im Sinne der Missachtung aussetzen könnte. Ich verspreche hiermit verbindlich, dass ich in keiner Weise Informationen oder Gegenstände, die dieser vereinbarten Schutzanordnung unterliegen, an andere Personen oder Organisationen weitergeben werde, es sei denn in strikter Übereinstimmung mit den Bestimmungen dieser Anordnung.

Ich erkläre mich ferner damit einverstanden, mich der Rechtsprechung des United States District Court for the Northern District of California zum Zwecke der Durchsetzung der Bestimmungen dieser vereinbarten Schutzanordnung zu unterwerfen, auch wenn ein solches Vollstreckungsverfahren nach Beendigung dieses Verfahrens stattfindet.

Ich bestimme hiermit _____ [vollständiger Name], wohnhaft in _____ [vollständige Adresse] als meinen kalifornischen Bevollmächtigten für die Zustellung von Schriftstücken im Zusammenhang mit dieser Klage oder einem Verfahren im Zusammenhang mit der Vollstreckung dieser vereinbarten Schutzanordnung.

Datum: _____

Stadt und Staat, in dem vereidigt und unterzeichnet wurde: _____

Name (gedruckt): _____

Unterschrift: _____

Mark L. Whitaker (*Pro Hac Vice*)

MWhitaker@mofo.com

Daniel P. Muino (Anwaltskammer Nr. 209624)

DMuino@mofo.com

G. Brian Busey (*Pro Hac Vice*) GBusey@mofo.com

Bradley S. Lui (Anwaltskammer Nr. 143088)

BLui@mofo.com

Mary Prendergast (Anwaltskammer Nr. 272737)

MPrendergast@mofo.com

Fahd H. Patel (*Pro Hac Vice*) FPatel@mofo.com

Bryan Wilson (Anwaltskammer Nr. 138842)

BWilson@mofo.com

Wendy Ray (Anwaltskammer Nr. 226269)

WRay@mofo.com

Jack W. Londen (Anwaltskammer Nr. 85776)

JLonden@mofo.com

Wesley E. Overson (Anwaltskammer Nr. 154737)

WOverson@mofo.com

Mathieu Swiderski (*Pro Hac Vice*) MSwiderski

@mofo.com

Michelle L. Yocum (*Pro Hac Vice*) MYocum@mofo.com

MORRISON & FOERSTER LLP

2000 Pennsylvania Avenue, NW

Washington, District of Columbia 20006-1888 Telefon:
+1.202.887.1500

*Anwälte für Teradata Corporation, Teradata US, Inc.,
und Teradata Operations, Inc.*

Tharan Gregory Lanier (Anwaltskammer Nr. 138784)

tglanier@JonesDay.com

Nathaniel P. Garrett (Anwaltskammer Nr. 248211)

ngarrett@JonesDay.com

Joshua L. Fuchs (*Pro Hac Vice*) jlfuchs@JonesDay.com

Joseph M. Beauchamp (*Pro Hac Vice*)

jbeauchamp@jonesday.com

JONES DAY

555 California Street, 26th Floor San Francisco, CA 94104

Telefon: +1.650.739.3941

Kenneth A. Gallo (*Pro Hac Vice*) kgallo@paulweiss.com

David J. Ball (*Pro Hac Vice*) dball@paulweiss.com

William B. Michael (*Pro Hac Vice*)

wmichael@paulweiss.com

Crystal M. Johnson (*Pro Hac Vice*)

cjohnson@paulweiss.com

PAUL WEISS

2001 K Street NW

Washington, DC 20006-1047

Telefon: +1.202.223.7356

Kristin L. Cleveland (Anwaltskammer Nr. 184639)

kristin.cleveland@klarquist.com

John D. Vandenberg (*Pro Hac Vice*)

john.vandenberg@klarquist.com KLARQUIST

SPARKMAN, LLP 121 SW Salmon Street, Suite 1600

Portland, OR 97204

Telefon: +1.503.595.5300

*Anwälte für SAP SE, SAP AMERICA, INC., und SAP LABS,
LLC*

BUNDESBEZIRKSGERICHT DER VEREINIGTEN STAATEN

NORTHERN DISTRICT OF CALIFORNIA

TERADATA CORPORATION, TERADATA US,
INC., und TERADATA OPERATIONS,

Kläger,

v.

SAP SE, SAP AMERICA, INC., und SAP LABS,
LLC,

Angeklagte.

Fall Nr. 3:18-CV-03670-WHO (JCS)

**VEREINBARTE ~~GEPLANTE~~
ÄNDERUNG DER SCHUTZANORDNUNG**

ANGESICHTS DER TATSACHE, dass Magistratsrichter Laporte am 14. Mai 2019 in diesem Fall die vereinbarte Schutzanordnung erließ. *Siehe* ECF Nr. 98.

ANGESICHTS DER TATSACHE, dass alle Parteien eingewilligt haben, Änderungen an der vereinbarten Schutzanordnung, wie sie hierin dargelegt werden, zu beantragen;

Demzufolge wird hiermit von und zwischen allen Parteien des Verfahrens festgelegt, dass die vereinbarte Schutzanordnung vorbehaltlich der Zustimmung des Gerichts wie folgt geändert werden soll:

- (1) Paragraph 7.4(c) wird geändert, indem am Ende dieses Abschnitts Folgendes hinzugefügt wird: "Sobald für den jeweiligen Experten eine Offenlegung erfolgt ist und die Einspruchsfrist abgelaufen ist oder Einsprüche zugunsten der Erlaubnis zur Offenlegung gegenüber dem Experten entschieden wurden, kann "Geschütztes Material" den Mitarbeitern und Assistenten eines Experten offengelegt werden, denen gegenüber die Offenlegung für diesen Rechtsstreit vertretbarerweise als notwendig erachtet wird. Vor der Offenlegung gegenüber dem Fachpersonal des Experten (in Abgrenzung zum Büropersonal) müssen diese Personen die "Anerkenntnis und Einverständnis, vertraglich gebunden zu sein" unterzeichnet haben.
- (2) Folgendes wird als Paragraph 8(f) der vereinbarten Schutzanordnung hinzugefügt: "(f) Verfahrensweise für ausführbare Software: Der Zugriff auf vereinbarte ausführbare Instanzen von Software darf nur Personen gewährt werden, die gemäß Paragraph 7.4 dieser vereinbarten Schutzanordnung die Berechtigung erhalten haben, Informationen einzusehen, die als "HOCH VERTRAULICH - NUR FÜR ANWÄLTE EINSEHBAR" und/oder "HOCH VERTRAULICH - QUELLCODE" eingestuft sind. Derartige ausführbare Software muss in einem Format zur Verfügung gestellt werden, das in der Lage ist, die beabsichtigte Standardfunktionalität der Software auszuführen, und muss die notwendigen technischen Geräte bereitstellen, die es der empfangenden Partei ermöglichen, diese Vorgänge durchzuführen. Die empfangende Partei darf Ausdrücke, Kopien oder anderweitige Aufzeichnungen der ausführbaren Software, wie Screenshots oder die Ergebnisse der an der ausführbaren Software durchgeführten Tests, anfertigen. Der unmittelbar vorangehende Satz gilt nicht für Quellcode (einschließlich ABAP-Code), auf den innerhalb der ausführbaren Instanzen zugegriffen werden kann. Das Vorgehen der empfangenden Partei in Bezug auf solchen Quellcode (einschließlich ABAP-Code) wird in der gleichen Weise eingeschränkt, wie in Absatz 8 dieser vereinbarten Schutzanordnung angegeben, und jeder Ausdruck eines solchen Quellcodes (einschließlich ABAP-Code) muss durch spezifische Anfragen an die vorlegende Partei, wie in Absatz 8 angegeben, erfolgen.

Die vorlegende Partei erteilt der empfangenden Partei die erforderlichen Zugriffsrechte, um die Funktionen, die mit der ausführbaren Software demonstriert werden sollen, ausführen und testen zu können. Die vorlegende Partei darf keine Protokolldateien erfassen oder auswerten, die die spezifischen Aktivitäten der empfangenden Partei nachweisen, es sei denn, dies ist für die Wartung der Software unbedingt erforderlich; in diesem Fall wird die empfangende Partei vor der Durchführung solcher Maßnahmen konsultiert. Die empfangende Partei ist jedoch verpflichtet, der vorlegenden Partei alle Daten, Datenstrukturen, Schemata und andere notwendige Informationen, auf die sich die empfangende Partei oder ihre Experten bei der Meinungsbildung oder Beweisführung in diesem Fall stützen oder die von der empfangenden Partei oder ihren Experten verwendet werden, in derselben Form zur Verfügung zu stellen, wie sie von der empfangenden Partei oder ihren Experten verwendet werden. Derartige Informationen müssen möglichst zeitnah zur Verfügung gestellt werden, damit die vorlegende Partei solche Handlungen oder Tests nachstellen kann, bevor sie die im Zusammenhang mit den Handlungen oder Tests geäußerten Standpunkte widerlegen muss. Die vorlegende Vertragspartei leistet angemessene technische Unterstützung, jedoch erst dann, wenn die empfangende Vertragspartei alle öffentlich zugänglichen Mittel zur eigenständigen Lösung technischer Fragen ausgeschöpft hat. Die Parteien kommen zusammen und beraten sich in guter Absicht, um Änderungen oder Ergänzungen dieser Beschränkungen und Schutzmaßnahmen vorzunehmen, wenn eine Partei feststellt, dass die Verwendung der ausführbaren Software nicht angemessen ist oder missbräuchlich verwendet wird."

Mit Datum vom: 21.
Oktober 2019

Hochachtungsvoll eingereicht,
MORRISON & FOERSTER LLP

Von: /s/ Mark L. Whitaker

Mark L. Whitaker

Mit Datum vom: 21.
Oktober 2019

Syndikus für Teradata Corporation, Teradata US,
Inc., und Teradata Operations, Inc.

JONES DAY

Von: /s/ Tharan Gregory Lanier

Tharan Gregory Lanier

Syndikus für SAP SE, SAP America, Inc., und
SAP Labs, LLC

GEMÄß DER BESTIMMUNG WIRD DIES SO ANGEORDNET:

Mit

Datum

vom: 21. Oktober 2019

[Stempel] UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

[Unterschrift] Judge Joseph C. Spero
Magistratsrichter